Solution Paper

Carrier-Grade Ethernet for Power Utilities

Ensuring Reliable Communications in the Smart Grid

RAD data communications

The Access Company

Abstract

Almost every power utility around the globe is either planning or has already begun the transformation of its T&D grid to an intelligent, packet-based network that can efficiently and reliably handle massive amounts of bi-directional or even multi-directional data communications between various devices and locations.

This paper reviews the various tools that carrier-grade Ethernet offers to meet the migration challenges that utilities are facing. It furthermore specifies the performance that is required from the ICT network, as well as discusses strategies that may be employed to implement the transition to Smart Grid communications.

Contents

1. Towards a Smarter Grid: Utility Networks in Transition

Power utility networks today are undergoing a revolutionary transformation: SDH/SONET infrastructure and legacy substation devices are being phased out to make way for Ethernet transport and IP/packet-based networks. The key driver for the transition to next generation communications is the move towards Smart Grids, as packet transport's high capacity and lower OpEx are required to handle the amount of bursty traffic generated by the advanced grid applications envisioned in intelligent power networks. IP SCADA systems (Ethernet Supervisory Control and Data Acquisition), wide area situation awareness (WASA) synchrophasor measurements and recent developments in substation automation (SA), such as the IEC 61850 standard are examples of new applications that mandate the use of packet switched networks and Ethernet capabilities throughout the transmission and distribution (T&D) grids. Other drivers include the use of high-resolution, IP-based video surveillance equipment, as well as wholesale and Utelco services providing broadband access for local businesses and service providers. Almost every power utility around the globe is either planning or has already begun the transformation of its T&D grid into an intelligent, packet-based network that can efficiently and reliably handle massive amounts of bi-directional or even multi-directional data communications between various devices and locations.

This trend is also evident from spending forecasts: According to a survey conducted by the Utilities Telecom Council (UTC) in 2011, Information Communications Technology (ICT) spending by US utility companies was estimated at $3.2 billion on telecommunications equipment and services; with spending on transport networks representing the second largest category following two-way metering[1]. According to a Pike Research study, equipment shipments for various Smart Grid applications, including distribution automation (DA) and substation automation in the WAN portion of the network, are expected to grow from 19 Million units in 2009 to nearly 103 Million in 2020[2].

In a 2012 survey among power utilities conducted by RAD, 24% of respondents reported that they have already started the migration process, while a similar rate reported their plan to do so within the next 12-24 months, and 16% over the next five years. Most (43%) of the respondents reported the communications network backbone as the first candidate for transition, while over 28% will begin with their SCADA system. Understandably, respondents were more hesitant about migrating their Teleprotection systems.

[1] Utilities Telecom Market Spending Forecast, UTC, 2011

[2] Smart Grid Networking and Communications Report, 2012, Pike Research - A Part of Navigant Consulting

The decision on which packet technology to use depends to a great extent on who is driving the transition within the utility organization. Those in charge of the distribution network, particularly the HAN (Home Area Network) and smart meters tend to prefer routable IP/MPLS as it enables a simpler addition of new devices to the network, while operations engineers find Layer 2 technology easier to manage in terms of bandwidth control, OAM, and security. Chapter 4 below reviews the various strengths and weaknesses of different packet technologies.

1.1 Migration Challenges and Communications Performance Requirements

While the migration to Smart Grid is probably unavoidable, utility companies, most of which operate self-owned, private networks, adopt a cautious approach to IP transformation. Traditionally a conservative segment, utility operators have been reluctant to migrate to IP without proper attributes to match TDM's deterministic behavior and high reliability. In particular, specific utility applications that require smart communications over packet-based networks need dependable service assurance tools to ensure low end-to-end delay, High Availability and resiliency. For example, the need for ultra-fast and reliable transmission in Teleprotection is translated to extremely low, symmetrical delay below 10 ms and minimal delay variation ("jitter"). Some SCADA applications, on the other hand, may tolerate latency levels as high as 1 second, while power quality Class A data needs 20ms (16.7 ms in 60 Hz networks) at most. Almost all applications require Four or Five Nines availability of 99.99% or 99.999%. Luckily, packet technologies – and specifically Ethernet – have matured enough so that they now include various mechanisms to guarantee the required performance levels, as described in the following chapter.

Another aspect that requires attention when introducing packet- and IP-based communications is cyber security. With the migration to Smart Grids, there is a sharp increase in the number of interconnected devices – the majority of which are located within consumer neighborhoods and homes where access is unrestricted. As a result, there is an increased number of potentially vulnerable entry points through which the grid can be disrupted. A critical infrastructure, power utility networks must therefore employ sophisticated and scalable security measures to prevent malicious attacks, as described later on in this paper.

The table below describes the levels of performance requirements for substation communication applications:

Attribute	Requirement	Comments
Bandwidth	Low, Medium, or High	Small distribution substations with basic SCADA systems, no video surveillance and no enterprise network access require little bandwidth, often served by 1200 baud[3] modems today. Larger substations acting as a hub for other backhaul networks, sophisticated protection switching, video surveillance, and enterprise communications require bandwidth as high as 100 Mbps to 1 Gbps.
Latency	Medium-Strict (end-to-end, in absolute terms and variability)	The most challenging communications is protection relay switching, which has very strict latency requirements – often less than 5 ms. Basic SCADA communications may not be inherently latency sensitive. Many of the vertically integrated legacy protocols assume direct Pt2Pt (if slow) links and many do not operate properly if encapsulated over networks with highly variable latency. Similarly, video communications generally require bounded latency.
Reliability	High	Significant harm might occur if connectivity were lost for a significant period of time (minutes to a few hours). Protection switching communications must be highly reliable. Failure to communicate a fault or switching event could cause significant failures in the grid. Basic SCADA monitoring is less sensitive, but the required reliability increases to the extent that control functions are expanded.
Security	High	Highly visible and widespread harm could result if link were intentionally compromised (i.e., data obtained or spoofed). Any misuse of the control network, deliberate or otherwise, could have very serious consequences. Many legacy SCADA systems have very poor security, which is compounded by the fact that much of the equipment is located in remote locations with limited physical security.

Source: Pike Research

Table 1: *Substation Automation communications requirements*

[3] Or, typically, 9600 baud

1.2 Traffic Types and Transmission Scenarios

The coexistence of newly-introduced IP connections and next-generation equipment with legacy infrastructure and substation devices results in two types of communications traffic that must be transmitted over the utility network:

- Ethernet and IP based data and signals from SA IEDs (Intelligent Electronic Devices)
- TDM-based traffic from existing equipment, e.g., analog voice, serial SCADA and Teleprotection signals

Newly deployed Ethernet/IP/MPLS networks offer a native communications environment for the former; however, the latter requires special mechanisms for delivery, such as pseudowire emulation (PWE). Other methods are expected to become available in the future, including direct mapping of payload to the Ethernet connection – thereby eliminating the TDM processing and pseudowire encapsulation phases – however currently, PWE is the prevailing method for delivering traffic between legacy devices in a packet-based environment.

Pseudowire emulation is an encapsulation method that allows a seamless connection by creating logical links, or virtual tunnels, between two elements across the packet network, while emulating the attributes of a TDM service, such as an E1, T1 or a fractional n x 64 kbps service.

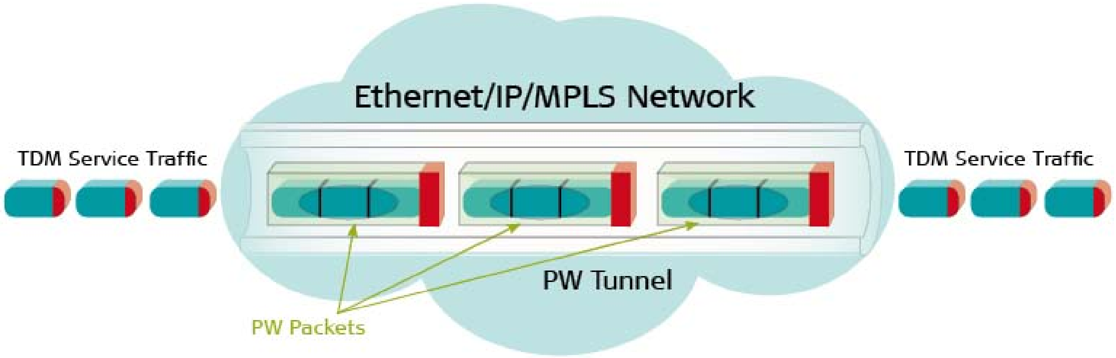

Figure 1: *TDM pseudowire emulation over packet networks*

The transmitted data streams are encapsulated in packets upon entering the network, and then reconstructed at the pseudowire egress, where clocking information is also regenerated. As a result, real-time traffic is delivered transparently without distortion, while avoiding the complexities of translating signaling data and ensuring that synchronization criteria are met. The latter issue is critical for legacy TDM devices, as the packet switched network is not synchronous, while TDM devices require a synchronized clock to function. The pseudowire emulation mechanism must therefore regenerate the original TDM timing accurately across the packet network.

The most common methods of TDM pseudowire emulation are based on the following standard protocols:

The **SAToP** (Structure Agnostic TDM over Packet) service treats the TDM traffic as a continuous data stream, ignoring any framing or timeslot channelization that may exist. It offers low bandwidth overhead, flexible packet sizes and low end-to-end delays; however, it is highly susceptible to frame loss, causing TDM end equipment to register faults and raise alarms when such loss occurs. In addition, SAToP is not bandwidth-optimized, as it requires a full E1/T1 capacity to transfer even a few timeslots.

CESoPSN (Circuit Emulation over PSN) supports framed and channelized TDM services. The packet must contain an integer multiple of the TDM frame or superframe, requiring a trade-off between low delay and low overhead. A CESoPSN payload always corresponds to 125 µs of TDM data, or some multiple thereof.

TDMoIP (TDM over IP), a standardized method developed by RAD, encapsulates TDM signals and supports unframed, framed and channelized TDM services. The packetization of TDM data is not performed according to the TDM frames, but rather by multiples of 48 Bytes. The resulting trade-off between delay and overhead might be unacceptable for some services.

Whichever method is ultimately selected to carry the TDM traffic, control and monitoring of pseudowire performance is also required while it traverses the packet network. A comprehensive set of carrier-grade Ethernet tools are used for this purpose, as described in the following chapter.

2. Carrier-grade Ethernet Mechanisms

Ethernet is no longer the LAN-oriented, connectionless-only technology it used to be, one that was associated with Best Effort performance. In recent years, concomitant with carriers pushing to deploy new services as revenue and growth generators, the industry engineered Ethernet into a technology with robust performance and tight control, backed by carrier-grade Service Level Agreements.

Consequently, a whole slew of standards has emerged, the result of work done by the IEEE (Institute of Electrical and Electronics Engineers), the MEF (Metro Ethernet Forum) and ITU-T (International Telecommunication Union – Telecommunications Standard Sector). The MEF, in particular, is an international industry consortium of carriers, service providers and telecom equipment vendors completely dedicated to the adoption of carrier-grade Ethernet. With performance guarantees, reliability schemes and service management tools in place, various carrier-grade Ethernet flavors have been extensively deployed as premium services with double-digit adoption rates world-wide. The following sections detail the different aspects of carrier-grade Ethernet that are relevant for power utility networks, including such features as Quality of Service guarantees, performance monitoring, fault management and resiliency.

2.1 Traffic Management and Quality of Service

Advancements in Ethernet technology allow the use of sophisticated mechanisms to provide mission-critical substation applications such as SCADA and IEC 61850 GOOSE (Generic Object Oriented Substation Events) messaging with the level of deterministic quality of service and priority they require. By managing bandwidth consumption and transmission priorities with CoS (Class of Service) granularity, multi-level hierarchical traffic management enables predictable latency and jitter performance across the service path. An advanced toolset includes the following:

Classification of incoming traffic into flows according to type and required QoS. Ethernet supports a wide variety of sorting criteria, such as VLAN-ID, Priority Code Point (PCP/P-bit) and MAC/IP address marking, to allow traffic identification in fine granularity. In this manner, SCADA protocols that operate over TCP/IP, such as IEC 60870-5-104, IEC 61850 and DNP3, can be classified according to L3/L4 characteristics (e.g., DSCP), whereas Ethernet-based 61850 GOOSE traffic can be handled per PCP, VLAN-ID L2 identifiers.

Metering and policing is applied for each flow to regulate traffic according to pre-defined CIR (Committed Information Rate) and EIR (Excess Information Rate) bandwidth profiles. Rate limiting is performed so that traffic is admitted into the network based on "color": Green (admitted frames), yellow ("Best-Effort" transmission), or red (discarded frames).

Hierarchical scheduling is used to define the order in which the various flows are forwarded, using a two-step scheduling mechanism so that each flow receives the desired priority. In this manner, higher priority traffic is serviced first, while still preventing lower-priority queues from being "starved". Advanced queue management techniques also serve for congestion avoidance purposes and to ensure minimal latency and jitter, even when a large amount of bursty traffic is sent over the same link.

Shaping to smooth out bursts and avoid buffer overruns in subsequent network elements.

Packet editing is employed to signal proper handling instructions for subsequent network elements and ensure data integrity.

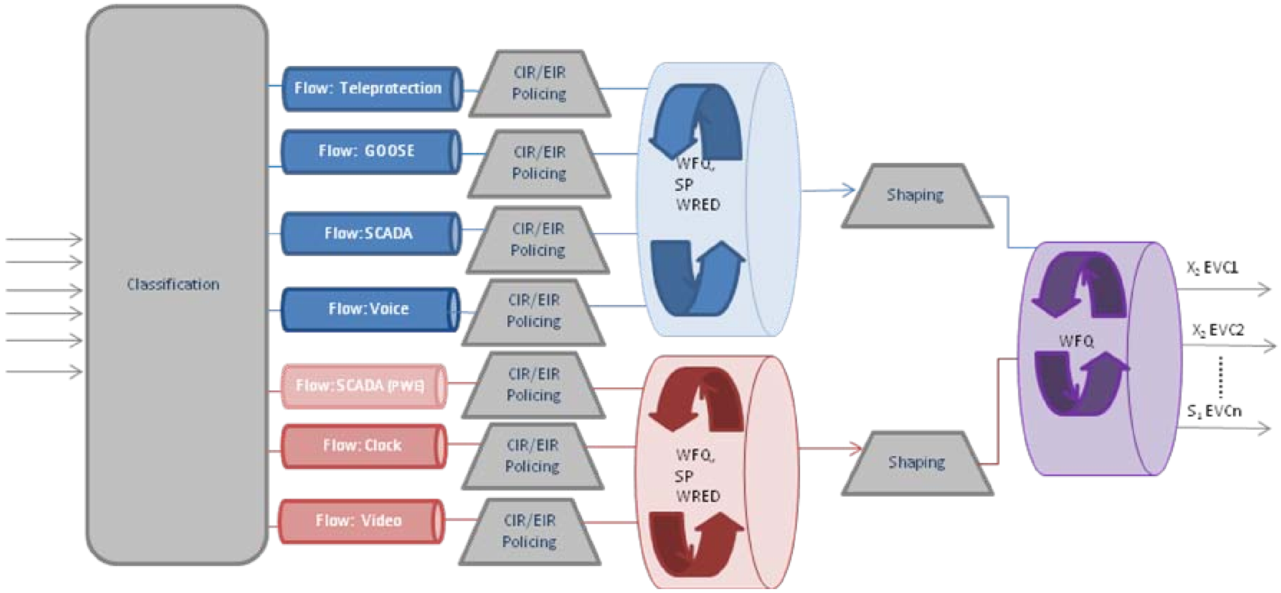

Figure 2: Packet-based traffic management and hierarchical QoS tools

2.2. Performance Monitoring and Testing

Carrier-grade Ethernet offers a wealth of tools to test, monitor and troubleshoot the operation of communications links. A comprehensive Ethernet OAM (operations, administration and maintenance) suite, delay, jitter, and packet loss measurement schemes, diagnostic loopbacks, and other means are available remotely, and automatically perform the following procedures:

- Connectivity verification
- Stress testing
- Performance monitoring
- Fault detection
- Fault propagation and isolation

Remote testing, end-to-end visibility and proactive monitoring capabilities help utility network operators anticipate service degradation ahead of time, as well as cut down truck-rolls and on-site technician calls, thereby ensuring consistent performance and lowering operational costs (OpEx).

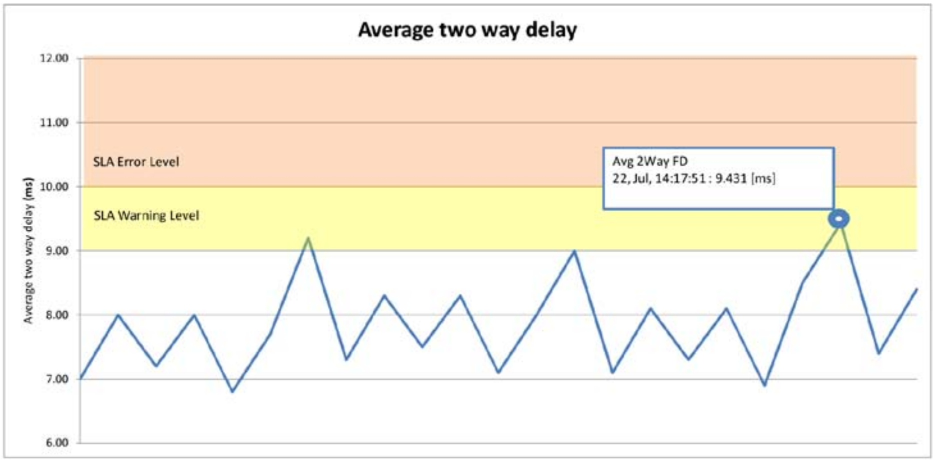

Figure 3: Ongoing monitoring for carrier-grade Ethernet's key performance indicators

2.3 Resiliency

Given their mission-critical nature, utility networks must be ensured fail-safe operation. From a communications perspective, resiliency can be achieved at a number of levels:

Hardware redundancy: Multiplexer resiliency should ideally be based on no single point of failure (NSPF) design with redundant, hot-swappable power supplies, as well as control plane card and switch fabric card redundancy.

Link redundancy: A typical mechanism is 1+1 protection topology with automatic switchover between links, which can compensate for network element or cable failure. Link aggregation group (LAG) can be used in worker/standby mode to move traffic from a failed link to a backup one.

Path protection: Carrier Ethernet standards provide various tools to ensure High Availability. These include Ethernet Linear Protection Switching (G.8031 ELPS) – also called "EVC (Ethernet Virtual Connection) protection" and Ethernet Ring Protection Switching (G.8032 ERPS) to provide Five Nines (99.999%) availability via service resiliency and speedy restoration.

3 Timing over Packet Synchronization

Packet switched networks were not designed with built-in synchronization mechanisms and therefore require complementary clock transfer solutions with a high level of precision to ensure a stable network with predictable performance. In utility networks, this is particularly required for supporting legacy equipment and for applications that are delay- and jitter-sensitive, such as protection, SCADA and power quality measurements (synchrophasors). While today's highest accuracy levels are in the 1ms zone, upcoming implementations of Smart Grid applications will require stringent 1µs (and even higher) accuracy. Up until recently, the prevailing custom entailed the use of a GPS at each node/service point; however, this approach poses several potentially problematic issues for utility network operators:

- Installing one or more GPS antennas on every RTU and communications device is costly, in terms of both CapEx and OpEx. It complicates the deployment process with the need for additional equipment and wiring, and wastes expensive technician time whenever the outdoor antenna requires maintenance;

- GPS is maintained and controlled by the U.S Department of Defense, which theoretically may choose to turn off the service selectively. Some organizations outside North America find the geopolitical implications of this unacceptable.

Other GNSS (global navigation satellite system) alternatives, such as the European Galileo project, the Russian GLONASS and the Chinese Beidou navigation system, are either not yet fully operational, do not offer the global coverage available by GPS and have similar potentially geopolitical weaknesses;

- A major problem is GPS jamming. As a passive radio element, a GPS receiver can be easily jammed using low-cost, readily available equipment. An active jammer can disrupt the operation of a utility terminal and even cause it to crash temporarily if operated in close enough proximity. This results in a security vulnerability that does not even require physical or virtual access to the network.

There are several methods in use today for ensuring synchronization in an all-packet environment. ITU-T's Synchronous Ethernet (Sync-E) methodology uses the Ethernet physical layer to accurately distribute frequency. Its operation thus requires unbroken support on every physical link along the path. Adaptive Clock Recovery (ACR) is another method of distributing frequency over a PSN, and relies on the packet arrival times of a TDM pseudowire stream, independent of the physical layer. IETF NTP and IEEE 1588-2008 Precision Time Protocol (PTP) exchange timestamp information in a master-slave hierarchy to deliver frequency and TOD (Time of Day) information, such as is needed for the proper operation of synchrophasors and to avoid cascading blackouts. PTP with on-path network support is a viable alternative to GPS for time synchronization.

Although PTP is capable of distributing both frequency and time, many network operators prefer to take advantage of the existing physical layer frequency distribution infrastructure (e.g. TDM or Synchronous Ethernet), and use the PTP service for time synchronization only. Furthermore, since many substation devices still use IRIG-B time codes, reliable conversion between PTP and IRIG-B is also a likely requirement in order to connect legacy equipment to the new Smart Grid.

IEC standard 61850 specifically addresses utility networks' needs in timing and synchronization over packet. It refers to IEEE C37.238 standard profile for use of IEEE Std. 1588 Precision Time Protocol in power system applications within substations and 1588 PTP Telco Profile across the WAN between substations.

Two main strategies are available for time distribution using PTP:

- Using a small number of Primary Reference Time Clocks (PRTCs)/PTP-Grandmasters (GMs) at the core/aggregation network, each servicing a large number of PTP-slave devices deployed at the base stations. The advantages of this approach include lower total cost of PRTCs/PTP-GMs (typically integrated into the same equipment) and an efficient fault protection scheme, as protection of each PRTC/PTP-GM covers many PTP-slaves. Its downside includes a relatively high number of intermediate network elements (e.g. switches and routers) with on-path support mechanisms – Boundary Clock (BC) and Transparent Clocks (TC) –required to combat the effect of Packet Delay Variation (PDV). It's important to note, however, that PTP allows network operators to opt for partial on-path support to limit the costs associated with deployment, provided that it delivers acceptable performance levels. Additional upgrades can be performed at a later stage to improve performance as needed.

- Using a large number of PRTCs/PTP-GMs at the core/aggregation network, each servicing a smaller number of PTP-slave devices deployed at the base stations. Positioning the PRTCs/PTP-GMs closer to the PTP-slaves results in much smaller time distribution chains and dramatically cuts the number of intermediate network elements that need to be enhanced with PTP on-path support. On the other hand, more PRTCs/PTP-GMs are now needed to cover the entire network. As PRTCs/PTP-GMs are typically large and expensive, this practice has immediate repercussions for the overall CapEx. Moreover, the PRTCs/PTP-GMs are now geographically dispersed (located closer to the network edges), making redundancy planning more complex and expensive, as in some cases a backup GM will be required at each site.

Another time distribution strategy – the "Hybrid GPS-PTP" – is being considered by operators who are willing to incorporate GPS in their networks, whereby PTP is used as backup in case the primary GPS fails.

Multi-generation utility communication devices that also support clock transfer enable substantive cost savings, as they eliminate the need for costly dedicated hardware and allow accurate monitoring of synchronization performance across the power system.

4 Choosing the Right Packet Network

Some power utilities are operating self-owned networks, while others lease some or all network services from a carrier or service provider. The preference for either approach tends to vary between regions according to regulatory, financial, cultural, and technological factors. According to Pike Research, the share of public wired technologies in utility networks "will decline, as traditional leased lines are replaced by newer and, in many cases, private, networking technologies. Private copper is projected to show a CAGR decline of nearly 18.2%, largely due to the use of new technologies (both wired and wireless), particularly with respect to SA and DA applications…fiber optic communications are projected to grow at about 7.9% on a CAGR basis, driven largely by utilities requiring higher substation bandwidth for applications including video surveillance systems at critical infrastructure points."[4]

Whether self-operated or leased from a carrier, a utility communications network must include the functionalities described above and, in the case of the latter, include performance guarantees in the form of an SLA (Service Level Agreement) purchased from the provider.

When migrating to next-gen networks, utility network operators need to choose which technology to employ, with available packet-based options including carrier-grade Ethernet, IP, vanilla MPLS (Multi-Protocol Label Switching), MPLS-TE, and the newest variant – MPLS-TP. In addition, they can consider utilizing the new generation of Circuit Switching (CS) based on OTNs (Optical Transport Networks). Like SDH/SONET, OTNs can be used as the physical layer for reliably transporting legacy and Ethernet or IP traffic over fiber optic connections at rates from 50 Mbps up to over 100 Gbps.

Each of the packet-based networks listed above can fulfill the basic aim of reliably transporting information from place to place, but have quite different characteristics:

IP is usually discussed in the context of the user information interface, but in some cases, it can be used as a transport network. The IP suite does not define lower layers, and thus must run over Ethernet, OTN, SDH/SONET (PoS – Packet over SDH/SONET), etc. Similarly, IP does not provide standard OAM or APS mechanisms, rather leveraging its native routing protocols. However, these are not always rapid enough to meet stringent availability requirements. IP has a strong security component called IPsec, which can provide authentication, integrity, and confidentiality mechanisms, but at a relatively high operational cost.

[4] Smart Grid Networking and Communications Report, 2012, Pike Research - A Part of Navigant Consulting

MPLS was originally devised as a method to accelerate IP forwarding, and to enable provisioning of QoS and VPN services for IP traffic. Being part of the IP suite, MPLS does not define lower layers, relying (like IP) on Ethernet, OTN, PoS, etc. MPLS did not originally have the OAM or APS mechanisms needed for a transport network, but these have been recently developed as part of the MPLS transport profile, known as MPLS-TP. MPLS was designed as a core network technology, and thus, like SDH/SONET and OTN, has very few security mechanisms. Although MPLS-TP enables MPLS to extend beyond the core, to date there has been little work on MPLS security.

Ethernet, as described earlier in this paper, was originally a LAN technology but has developed into a carrier-grade network with OAM and APS features. While Ethernet defines a native physical layer from 10 Mbps up to 100 Gbps, Ethernet frames can also be transported over other physical layers (e.g., OTN) and over MPLS via pseudowires. Ethernet has several security-specific features, including the widely implemented IEEE 802.1X and emerging MACsec (see Chapter 5: Security for further information).

The following table summarizes the strengths and weaknesses in security, resiliency and operations of the main packet technologies:

Protocol	OAM/APS	Security
IP	No standard end-to-end mechanisms	Strong (IPsec)
MPLS	Recently developed for MPLS-TP	No built-in security
Ethernet	Carrier-grade	Several security mechanisms defined (802.1X, MACsec)

Table 2: *Key feature comparison for packet technologies*

The decision on which packet technology to implement depends on a number of factors, among which are the number of sites to be connected and their size, as well as on the ability of the selected solution to ensure consistent performance across the different access media available at each site.

While an end-to-end VPLS (Virtual Private LAN Service based on Ethernet over MPLS) can provide the required resiliency for critical applications by using a low-latency Fast Re-Route (FRR) protection mechanism, it has severe security issues, limited built-in OAM tools for performance monitoring in the network and prohibitive per-port costs in large deployments. A combination of Layer 2 Ethernet access with an MPLS core, on the other hand, offers lower cost per port, richer OAM and PM tools for native Layer 2 Ethernet connections and advanced protection mechanisms via Ethernet Ring Protection Switching and Ethernet Linear Protection Switching. In addition, it allows utility network operators to maintain their existing access media installed base, and may be an optimal fit for a large number of distributed sites with copper, fiber and wireless infrastructure.

An example for such a combination is illustrated in the use of a L2 technology in the access and aggregation portions of the network, so that GOOSE messages can be delivered **between** substations without traversing an MPLS core. The IEC 61850 standard sets performance requirements for the delivery of GOOSE messages over the WAN. Since these messages are Ethernet-based, many find the use of a Layer 2 technology the most efficient transport method, as it is simpler and eliminates the need for tunneling or L2 to L3 conversion, which adds to end-to-end delay. This is true, provided that performance can be effectively monitored and guaranteed, using the tools described above.

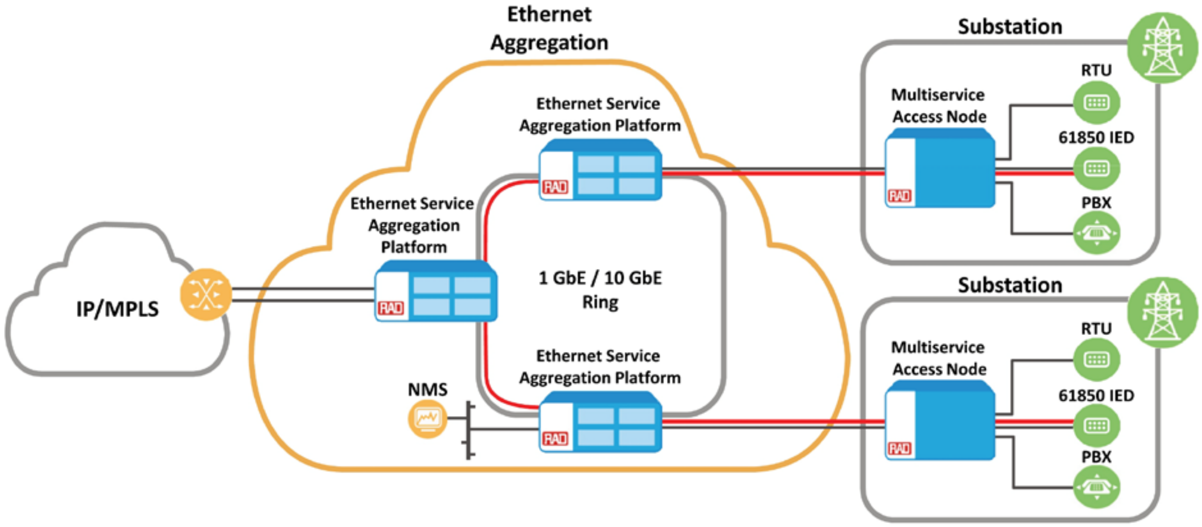

Figure 4: Combining IP/MPLS core with carrier-grade Ethernet access and aggregation

5 Security

While in silo-based legacy networks security hasn't been considered much of an issue, modern industrial automation networks that use Ethernet- and IP-based infrastructure, and which consist of many inter-connected devices, are much more vulnerable to cyber attacks and therefore need to implement proper protection measures. The various security protocols mentioned in the previous chapter provide only a partial solution, as a more effective approach in the case of public utilities should be a layered, "Defense in Depth" one, in which multiple levels of protection are implemented. Ideally, such a comprehensive set of security tools can be deployed in the network without adding too many dedicated security appliances on top of the communications infrastructure. The following describes the elements that make up a multi-layered security strategy in a utility network:

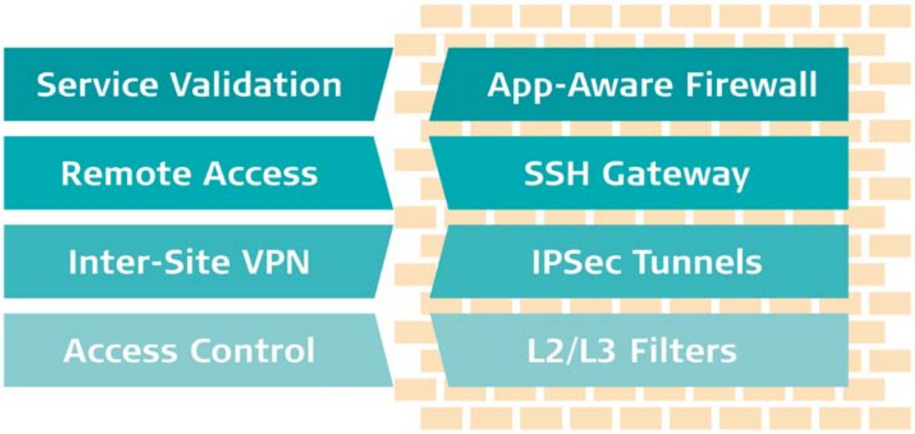

Figure 5: Defense in Depth with multiple security layers

5.1 Network Access Control

The first level of security is based on physical authentication of the devices connecting to the network according to their MAC or IP address. As mentioned above, carrier-grade Ethernet today offers several mechanisms to protect against various forms of attacks. One of them is IEEE 802.1x, an authentication protocol for point-to-point links, enabling dynamic management of access authorization based on user identities. Alternatively, ACL (Access List) rules can be configured per switch port, to allow only devices with specific MAC or IP addresses to be admitted.

5.2 Inter-Site VPN

Some distributed networks, – those of a nationwide utility, for example – may need to use public infrastructure leased lines (3G, DSL, etc.), to connect between remote sites. The integrity of the data that is transmitted using such inter-site connectivity must be protected; and often encryption is also required to ensure confidentiality. When the data is inherently L3, an IPsec gateway is employed to form an IPsec Virtual Private Network (VPN). Alternatively, Ethernet MACsec (IEEE 802.1AE) may be used for source authentication, integrity protection and optionally confidentiality, without the need for deploying a security gateway. In addition, GRE tunneling enables transparent connection of sites, forming a single Ethernet network without the need for the logistics of IP addressing and routing logic. The use of IPSec in conjunction with GRE enables the preservation of service-defining VLAN information.

5.3 Secure Remote Access

When a remote user needs to access a secure network for operational or maintenance tasks, it is critical to ensure that only a limited set of authorized activities are enabled and performed in a strictly secure manner. When remote access is initiated by an individual from an unknown location, a VPN connection as described above may be too vulnerable. Instead, a more controlled tunnel with limited access rights should be used. An SSH (Secure Shell) server located at a secure site enables such limited remote access for operations and maintenance, e.g., Telnet and management applications, by allowing remote users, such as field technicians, to log in over an encrypted communications channel. Regarding network management traffic, security is provided by the SNMPv3 protocol, which is considered standard for critical and/or sensitive systems.

5.4 Application-Aware Firewall

Due to the unique characteristics of industrial applications, existing security concepts from the enterprise world – such as the centralized firewall approach – are not necessarily effective, as anyone with access to a connected device in the internal network can hack into the entire grid. By deploying Ethernet switches with an integrated firewall on each port, utility operators can implement a distributed, network-based security solution that is equivalent to the use of personal firewalls on each system or device within the network. These service- and application-aware firewalls are used to validate the application logic as represented in the communication flow between all devices in the network, defining, for example, specific allowed functions in the SCADA protocol layer. This "white listing" philosophy is more suitable for utility networks than the "black listing" measures used to block malicious programs in the enterprise world, as it of based on a finite, known list of applications and functions.

6 RAD's Carrier-Grade Ethernet Solutions for Power Utilities

Megaplex

Multiservice Access Platforms

ETX-A

Carrier Ethernet over Fiber

IPmux

TDM Pseudowire Gateway

ETX-5300A

Multiservice Aggregation Platform

RIC-GE

Gigabit Ethernet over SDH

RADiFlow

Service-Aware Secure

Ethernet Switches

Figure 6: RAD's carrier-grade Ethernet solutions – enabling a smooth migration

RAD's best-of-breed, hybrid SDH/SONET and PSN access solutions for the energy market allow utilities to choose the migration path that best suits their needs. By combining carrier-grade Ethernet capabilities with extensive support for legacy services and interfaces, RAD's system solution offer the following benefits:

- Easy integration of intelligent electronic devices (IEDs) and Smart Grid services and equipment over existing TDM infrastructure

- Service continuity for legacy applications and equipment, even after core networks are replaced to Ethernet/IP/MPLS
- Circuit emulation solutions without compromising service quality or latency levels
- Ensure deterministic QoS for NGN services and advanced grid applications over packet transport using multi-priority traffic management, end-to-end OAM and diagnostics, and performance monitoring
- Multi-standard timing over packet synchronization, including 1588 Grandmaster functionality in the same communications device
- Multi-level redundancy options for Five Nines resiliency
- Future-proof solutions streamlined for Smart Grid communications and IEC61850 architecture, including reliable, low-latency Ethernet services between sites with real-time messaging, such as GOOSE/GSSE
- Help protect critical infrastructure and IP-based SCADA systems from malicious cyber attacks with cyber security and authentication protocols, such as SSH, SSL, SNMPv3, and RADIUS

Among the various options offered to utility network operators, RAD's hybrid solutions enable the use of a single device to migrate non-critical services to the new packet environment, while protection and other vital traffic is kept over the legacy SDH/SONET network for the duration of the transition period with a roll back option, thus allowing a phased transition without increasing the capital investment or operating costs involved in the process.

Conclusion

The move towards Smart Grids and next-generation networks in utility communications is already under way, requiring utilities to give special attention to their critical applications. Robust clock accuracy, QoS assurance, resiliency, and on-going performance monitoring are "must have" elements in any next-generation network being considered by utility network operators.

To meet specific utility needs and challenges, a typical smart utility communications network should include the following elements/capabilities:

- Support for legacy services and traffic

- Traffic management and hard/hierarchical QoS
- Synchronization
- Security

Utilities around the world are discovering that Ethernet has been engineered and standardized with exactly such qualities to become carrier-grade, and are now thus capable of meeting the exacting requirements of critical utility applications. While several packet-based networking options are available, a comparison between them outlines their respective strong and weak points. A combination of carrier-grade Ethernet in the access/aggregation with an MPLS core may, in many cases, satisfy these requirements while addressing the needs of various functions within the utility organization.

Utilities may operate on different schedules with regards to the move to smart communications, however they all share the need to lower migration costs and make it as efficient as possible. RAD Data Communications helps them achieve exactly that with a wide selection of utility-grade solutions, from multi-functional devices, providing the highest performance while optimizing the number of network elements to be deployed, to hybrid TDM/Packet solutions, which allow utility operators the freedom to choose the migration path that best suits their needs and budgets.

www.rad.com

International Headquarters
RAD Data Communications Ltd.
24 Raoul Wallenberg St.
Tel Aviv 69719 Israel
Tel: 972-3-6458181
Fax: 972-3-6498250
E-mail: market@rad.com
www.rad.com

North America Headquarters
RAD Data Communications Inc.
900 Corporate Drive
Mahwah, NJ 07430 USA
Tel: (201) 529-1100,
Toll free: 1-800-444-7234
Fax: (201) 529-5777
E-mail: market@radusa.com
www.radusa.com

RAD
data communications
The Access Company

Catalog no. 802544 Version 7/2012